Claims

What is claimed is:

1. An authenticated identity translation method comprising:

establishing an authenticated user identity responsive to an identification and authentication event within a domain comprising an initial authentication unit and a subsequent authentication unit, said identification and authentication event occurring at said initial authentication unit, said initial authentication unit and said subsequent authentication unit employing disparate user registries with different user identities;

generating a token representative of said identification and authentication event to be forwarded to said subsequent authentication unit; and

translating the authenticated user identity of said initial authentication unit to a local user identity of said subsequent authentication unit, wherein said subsequent authentication unit initiates said translating employing said token.

2. The method of claim 1, wherein the domain further comprises a domain controller, and wherein said method further comprises forwarding said token from said subsequent authentication unit to said domain controller, and said translating further comprises using said token to translate by the domain controller the authenticated user identity to the local user identity, wherein said translating includes employing a global registry of said different user identities maintained by the domain controller to translate the authenticated user identity into the local user identity for the subsequent authentication unit.

3. The method of claim 2, wherein the token comprises a translation token, said translation token including at least some of an identity of the initial authentication unit, a user identity, a method of authentication employed, and a time stamp representative of time of authentication.

4. The method of claim 3, wherein said generating further comprises obtaining signing value pair information from the domain controller, and signing the translation token using said signing value pair.

5. The method of claim 4, wherein said translating by the domain controller further comprises validating the translation token signature prior to said translating of the authenticated user identity to the local user identity using the global registry of different user identities.

6. The method of claim 5, wherein said signing value pair comprises a signing value and a sequence number, and wherein said sequence number is encrypted by the domain controller employing an encryption key known only to the domain controller, and said validating includes employing the encryption key to validate the translation token.

7. The method of claim 3, wherein said generating further comprises providing the translation token to the domain controller, storing the translation token by the domain controller and obtaining a token reference, said token reference comprising an index to said stored translation token of the domain controller, wherein said forwarding and said translating employ said token reference.

8. The method of claim 7, wherein said translating further comprises employing said token reference to retrieve said translation token by the domain controller, and thereafter using said translation token to find the local user identity in the global registry of different user identities.

9. The method of claim 2, further comprising authenticating the local user identity at the subsequent authentication unit, said authenticating being based on a return code received from the domain controller with the local user identity, said return code being based on at least one authentication policy for the domain.

10. The method of claim 9, wherein said at least one authentication policy is at least one of user dependent or method of authentication dependent for said subsequent authentication unit, and wherein the method of authentication comprises a method of authentication employed by said establishing of said authenticated user identity at said initial authentication unit.

11. The method of claim 2, further comprising repeating said method for at least one additional subsequent authentication unit, wherein with each repeating, said subsequent authentication unit becomes said initial authentication unit and said at least one additional subsequent authentication unit becomes said subsequent authentication unit, wherein said domain controller is employed by each at least one additional subsequent authentication unit in translating the token to a respective local user identity.

12. The method of claim 2, wherein said generating occurs at said initial authentication unit.

13. The method of claim 1, wherein the domain comprises a trust domain, and wherein the method further comprises initially establishing said trust domain within which the authenticated identity translation is to occur.

14. The method of claim 1, wherein said initial authentication unit comprises an initial server, and said subsequent authentication unit comprises at least one subsequent server, wherein the at least one subsequent server receives a request from the initial server, along with said token.

15. The method of claim 14, wherein said method further comprises forwarding the request and the token to multiple subsequent servers.

16. The method of claim 1, wherein said method further comprises one of forwarding the token to the subsequent authentication unit directly from the initial authentication unit or forwarding the token from the initial authentication unit through a user of the initial authentication unit to the subsequent authentication unit.

17. The method of claim 1, wherein the initial authentication unit and the subsequent authentication unit reside in different partitions of a multi-partition computing environment.

18. The method of claim 1, wherein the initial authentication unit is also another subsequent authentication unit to a further initial authentication unit establishing another authenticated user identity.

19. The method of claim 18, wherein the subsequent authentication unit comprises said further initial authentication unit.

20. The method of claim 1, further comprising repeating said method for multiple users, employing multiple initial authentication units, each requiring access to at least one subsequent authentication unit.

21. The method of claim 1, wherein said domain comprises a heterogeneous computing network, and wherein said initial authentication unit and said subsequent authentication unit comprise heterogeneous computing units.

22. The method of claim 1, wherein the domain further comprises a domain controller, and wherein said translating further comprises using said token to translate by the domain controller the authenticated user identity to the local user identity, wherein the domain controller functions as a server and the initial authentication unit and subsequent authentication unit function as clients in a client/server based model.

23. The method of claim 1, wherein the generating further comprises securing the token against modification prior to said forwarding of the token to said subsequent authentication unit.

24. The method of claim 1, wherein a structure of said token is programmable by an administrator of said domain.

25. The method of claim 1, wherein the domain further comprises a domain controller, and wherein said method further comprises performing by the domain controller at least one of retiring the token or purging the token subsequent to said translating.

26. The method of claim 1, wherein said method further comprises employing a secure protocol to transfer a request and said token from said initial authentication unit to said subsequent authentication unit.

27. An authenticated identity translation system comprising:

means for establishing an authenticated user identity responsive to an identification and authentication event within a domain comprising an initial authentication unit and a subsequent authentication unit, said identification and authentication event occurring at said initial authentication unit, said initial authentication unit and said subsequent authentication unit employing disparate user registries with different user identities;

means for generating a token representative of said identification and authentication event to be forwarded to said subsequent authentication unit; and

means for translating the authenticated user identity of said initial authentication unit to a local user identity of said subsequent authentication unit, wherein said subsequent authentication unit initiates said translating employing said token.

28. The system of claim 27, wherein the domain further comprises a domain controller, and wherein said system further comprises means for forwarding said token from said subsequent authentication unit to said domain controller, and said means for translating further comprises means for using said token to translate by the domain controller the authenticated user identity to the local user identity, wherein said means for translating includes means for employing a global registry of said different user identities maintained by the domain controller to translate the authenticated user identity into the local user identity for the subsequent authentication unit.

29. The system of claim 28, wherein the token comprises a translation token, said translation token including at least some of an identity of the initial authentication unit, a user identity, a method of authentication employed, and a time stamp representative of time of authentication.

30. The system of claim 29, wherein said means for generating further comprises means for obtaining signing value pair information from the domain controller, and for signing the translation token using said signing value pair.

31. The system of claim 30, wherein said means for translating by the domain controller further comprises means for validating the translation token signature prior to translating of the authenticated user identity to the local user identity using the global registry of different user identities.

32. The system of claim 31, wherein said signing value pair comprises a signing value and a sequence number, and wherein said sequence number is encrypted by the domain controller employing an encryption key known only to the domain controller, and said means for validating includes means for employing the encryption key to validate the translation token.

33. The system of claim 29, wherein said means for generating further comprises means for providing the translation token to the domain controller, means for storing the translation token by the domain controller and means for obtaining a token reference, said token reference comprising an index to said stored translation token by the domain controller, wherein said means for forwarding and said means for translating employ said token reference.

34. The system of claim 33, wherein said means for translating further comprises means for employing said token reference to retrieve said translation token by the domain controller, and thereafter for using said translation token to find the local user identity in the global registry of different user identities.

35. The system of claim 28, further comprising means for authenticating the local user identity at the subsequent authentication unit, said authenticating being based on a return code received from the domain controller with the local user identity, said return code being based on at least one authentication policy for the domain.

36. The system of claim 35, wherein said at least one authentication policy is at least one of user dependent or method of authentication dependent for said subsequent authentication unit, and wherein the method of authentication comprises a method of authentication employed by said means for establishing of said authenticated user identity at said initial authentication unit.

37. The system of claim 28, further comprising means for repeating said system for at least one additional subsequent authentication unit, wherein with each repeating, said subsequent authentication unit becomes said initial authentication unit and said at least one additional subsequent authentication unit becomes said subsequent authentication unit, wherein said domain controller is employed by each at least one additional subsequent authentication unit in translating the token to a respective local user identity.

38. The system of claim 28, wherein said means for generating occurs at said initial authentication unit.

39. The system of claim 27, wherein the domain comprises a trust domain, and wherein the system further comprises means for initially establishing said trust domain within which the authenticated identity translation is to occur.

40. The system of claim 27, wherein said initial authentication unit comprises an initial server, and said subsequent authentication unit comprises at least one subsequent server, wherein the at least one subsequent server receives a request from the initial server, along with said token.

41. The system of claim 40, wherein said system further comprises means for forwarding the request and the token to multiple subsequent servers.

42. The system of claim 27, wherein said system further comprises one of means for forwarding the token to the subsequent authentication unit directly from the initial authentication unit or means for forwarding the token from the initial authentication unit through a user of the initial authentication unit to the subsequent authentication unit.

43. The system of claim 27, wherein the initial authentication unit and the subsequent authentication unit reside in different partitions of a multi-partition computing environment.

44. The system of claim 27, wherein the initial authentication unit is also another subsequent authentication unit to a further initial authentication unit establishing another authenticated user identity.

45. The system of claim 44, wherein the subsequent authentication unit comprises said further initial authentication unit.

46. The system of claim 27, further comprising means for repeating said system for multiple users, employing multiple initial authentication units, each requiring access to at least one subsequent authentication unit.

47. The system of claim 27, wherein said domain comprises a heterogeneous computing network, and wherein said initial authentication unit and said subsequent authentication unit comprise heterogeneous computing units.

48. The system of claim 27, wherein the domain further comprises a domain controller, and wherein said means for translating further comprises means for using said token to translate by the domain controller the authenticated user identity to the local user identity, wherein the domain controller functions as a server and the initial authentication unit and subsequent authentication unit function as clients in a client/server based model.

49. The system of claim 27, wherein the means for generating further comprises means for securing the token against modification prior to said forwarding of the token to said subsequent authentication unit.

50. The system of claim 27, wherein a structure of said token is programmable by an administrator of said domain.

51. The system of claim 27, wherein the domain further comprises a domain controller, and wherein said system further comprises means for performing by the domain controller at least one of retiring the token or purging the token subsequent to said translating.

52. The system of claim 27, wherein said system further comprises means for employing a secure protocol to transfer a request and said token from said initial authentication unit to said subsequent authentication unit.

53. An authenticated identity translation system comprising:

a trusted domain comprising an initial authentication unit, a subsequent authentication unit, and a domain controller, said initial authentication unit and said subsequent authentication unit employing disparate user registries with different user identities;

said initial authentication unit being adapted to establish an authenticated user identity responsive to an identification and authentication event occurring thereat, and to generate a token representative of said identification and authentication event to be forwarded to said subsequent authentication unit; and

said subsequent authentication unit being adapted to forward said token to the domain controller for translating the authenticated user identity of said initial authentication unit to a local user identity of said subsequent authentication unit, wherein said translating includes employing said token received from said initial authentication unit.

54. At least one program storage device readable by a machine, tangibly embodying at least one program of instructions executable by the machine to perform an authenticated identity translation method, said method comprising:

establishing an authenticated user identity responsive to an identification and authentication event within a domain comprising an initial authentication unit and a subsequent authentication unit, said identification and authentication event occurring at said initial authentication unit, said initial authentication unit and said subsequent authentication unit employing disparate user registries with different user identities;

generating a token representative of said identification and authentication event to be forwarded to said subsequent authentication unit; and

translating the authenticated user identity of said initial authentication unit to a local user identity of said subsequent authentication unit, wherein said subsequent authentication unit initiates said translating employing said token.

55. The at least one program storage device of claim 54, wherein the domain further comprises a domain controller, and wherein said method further comprises forwarding said token from said subsequent authentication unit to said domain controller, and said translating further comprises using said token to translate by the domain controller the authenticated user identity to the local user identity, wherein said translating includes employing a global registry of said different user identities maintained by the domain controller to translate the authenticated user identity into the local user identity for the subsequent authentication unit.

56. The at least one program storage device of claim 55, wherein the token comprises a translation token, said translation token including at least some of an identity of the initial authentication unit, a user identity, a method of authentication employed, and a time stamp representative of time of authentication.

57. The at least one program storage device of claim 56, wherein said generating further comprises obtaining signing value pair information from the domain controller, and signing the translation token using said signing value pair.

58. The at least one program storage device of claim 57, wherein said translating by the domain controller further comprises validating the translation token signature prior to said translating of the authenticated user identity to the local user identity using the global registry of different user identities.

59. The at least one program storage device of claim 58, wherein said signing value pair comprises a signing value and a sequence number, and wherein said sequence number is encrypted by the domain controller employing an encryption key known only to the domain controller, and said validating includes employing the encryption key to validate the translation token.

60. The at least one program storage device of claim 56, wherein said generating further comprises providing the translation token to the domain controller, storing the translation token by the domain controller and obtaining a token reference, said token reference comprising an index to said stored translation token of the domain controller, wherein said forwarding and said translating employ said token reference.

61. The at least one program storage device of claim 60, wherein said translating further comprises employing said token reference to retrieve said translation token by the domain controller, and thereafter using said translation token to find the local user identity in the global registry of different user identities.

62. The at least one program storage device of claim 55, further comprising authenticating the local user identity at the subsequent authentication unit, said authenticating being based on a return code received from the domain controller with the local user identity, said return code being based on at least one authentication policy for the domain.

63. The at least one program storage device of claim 62, wherein said at least one authentication policy is at least one of user dependent or method of authentication dependent for said subsequent authentication unit, and wherein the method of authentication comprises a method of authentication employed by said establishing of said authenticated user identity at said initial authentication unit.

64. The at least one program storage device of claim 55, further comprising repeating said method for at least one additional subsequent authentication unit, wherein with each repeating, said subsequent authentication unit becomes said initial authentication unit and said at least one additional subsequent authentication unit becomes said subsequent authentication unit, wherein said domain controller is employed by each at least one additional subsequent authentication unit in translating the token to a respective local user identity.

65. The at least one program storage device of claim 55, wherein said generating occurs at said initial authentication unit.

66. The at least one program storage device of claim 54 , wherein the domain comprises a trust domain, and wherein the method further comprises initially establishing said trust domain within which the authenticated identity translation is to occur.

67. The at least one program storage device of claim 54, wherein said initial authentication unit comprises an initial server, and said subsequent authentication unit comprises at least one subsequent server, wherein the at least one subsequent server receives a request from the initial server, along with said token.

68. The at least one program storage device of claim 67, wherein said method further comprises forwarding the request and the token to multiple subsequent servers.

69. The at least one program storage device of claim 54, wherein said method further comprises one of forwarding the token to the subsequent authentication unit directly from the initial authentication unit or forwarding the token from the initial authentication unit through a user of the initial authentication unit to the subsequent authentication unit.

70. The at least one program storage device of claim 54, wherein the initial authentication unit and the subsequent authentication unit reside in different partitions of a multi-partition computing environment.

71. The at least one program storage device of claim 54, wherein the initial authentication unit is also another subsequent authentication unit to a further initial authentication unit establishing another authenticated user identity.

72. The at least one program storage device of claim 71, wherein the subsequent authentication unit comprises said further initial authentication unit.

73. The at least one program storage device of claim 54 , further comprising repeating said method for multiple users, employing multiple initial authentication units, each requiring access to at least one subsequent authentication unit.

74. The at least one program storage device of claim 54, wherein said domain comprises a heterogeneous computing network, and wherein said initial authentication unit and said subsequent authentication unit comprise heterogeneous computing units.

75. The at least one program storage device of claim 54, wherein the domain further comprises a domain controller, and wherein said translating further comprises using said token to translate by the domain controller the authenticated user identity to the local user identity, wherein the domain controller functions as a server and the initial authentication unit and subsequent authentication unit function as clients in a client/server based model.

76. The at least one program storage device of claim 54, wherein the generating further comprises securing the token against modification prior to said forwarding of the token to said subsequent authentication unit.

77. The at least one program storage device of claim 54, wherein a structure of said token is programmable by an administrator of said domain.

78. The at least one program storage device of claim 54, wherein the domain further comprises a domain controller, and wherein said method further comprises performing by the domain controller at least one of retiring the token or purging the token subsequent to said translating.

79. The at least one program storage device of claim 54, wherein said method further comprises employing a secure protocol to transfer a request and said token from said initial authentication unit to said subsequent authentication unit.

* * * * *